

The complaint

Mr C is unhappy that Think Money Limited (“thinkmoney”) hasn’t reimbursed him for his loss after he was the victim of a scam.

What happened

On 6 September 2021 Mr C received an email he believed to be from a builder he’d employed to work on his home. His son had been speaking to the builder for some time at this point arranging the work they were due to carry out. The email asked him to make a payment of £10,000 before work would commence the next day.

Mr C tried to make the payment online but was locked out of his account due to him using the incorrect security information. He called thinkmoney to make the transfer which allowed him to make it using an alternative security process as a one off. During this call, thinkmoney asked Mr C questions about what the payment was for and who it was to.

After the payment had been made Mr C’s son received a message from the builder. They told Mr C their email account had been hacked and they could see someone had sent emails from the account and then deleted them. They established Mr C had been the victim of an email intercept scam, where a scammer had pretended to be the builder and had requested the deposit was paid to their account instead of the builder’s. The £10,000 Mr C had sent had been paid to the scammer.

Mr C reported the matter to thinkmoney, but it didn’t feel it was liable for Mr C’s loss as he’d authorised the payment and it had followed his instructions. But, it acknowledged there was a significant delay in acknowledging his complaint and offered him £50 for this.

Mr C brought the complaint to our service and our investigator upheld it. They felt thinkmoney ought to have recognised that Mr C was the victim of a common scam when it spoke to him and prevented it from being made. Thinkmoney didn’t accept this. It said email intercept scams weren’t common and it couldn’t have recognised Mr C was the victim of a scam based on its conversation with him.

As thinkmoney didn’t accept the investigator’s findings, the complaint has been passed to me to make a decision.

What I’ve decided – and why

I’ve considered all the available evidence and arguments to decide what’s fair and reasonable in the circumstances of this complaint.

The relevant law and regulations – plus good industry practice and thinkmoney’s own terms and conditions – suggest it has a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible. It might be negligent and liable for

reasonably foreseeable losses if, in breach of that duty of care, it fails to act on information which ought reasonably alert an authorised payment institution to potential fraud or financial crime by, or against its customer.

But, the Payment Services Regulations 2017, alongside thinkmoney's own terms and conditions, also indicate it should execute and authorise payment instructions without undue delay. And as a starting point there is a presumption that liability for authorised payments is on the payer, even where it might've been made as part of a scam.

There's no dispute in this case that Mr C authorised the payment to the scammer. But thinkmoney has confirmed the payment was picked up by its fraud team. When Mr C contacted it by phone to make the payment due to an unrelated issue, thinkmoney, in line with its fraud prevention processes, carried out some checks with Mr C before it allowed the payment to be made. As it's not in dispute thinkmoney recognised the payment as a potential risk, it's for me to decide whether I think thinkmoney did enough when it spoke to Mr C to satisfy itself the payment was genuine.

As part of the additional fraud checks carried out by thinkmoney, Mr C was asked who the payment was going to, he confirmed his builder, and he was asked if he'd paid them before, he confirmed he hadn't. He was then asked where the money had come from, which he answered. I'm satisfied these questions were part of its fraud processes, because it didn't need to know this information in order to follow his payment instruction.

I don't think these questions went far enough for thinkmoney to reasonably satisfy itself Mr C was not the victim of a scam. It's clear Mr C believed he was making payment to a builder, but I would've expected thinkmoney to go further in asking him what contact he'd had with the builder, how he'd received their payment details and if they'd recently changed.

I say this because email intercept scams are common and well recognised scams where an individual receives an email they believe to be from a supplier asking for payment, but the bank details provided are the scammers. And I'd expect thinkmoney to be aware of, and on the look out for common scams such as this one and ask relevant questions related to how this type of scam tends to be perpetrated. Upon identifying a scam risk as it ought to have done here, I would've expected it to have provided information and warnings about how this type of scam tends to work and how Mr C could best protect himself. For example, when it established Mr C had only received payment details via email, I would've expected it to recommend he contact the builder directly to confirm and I would've expected it to explain why.

Thinkmoney has argued that email intercept or invoice scams aren't common. It feels it isn't reasonable to suggest it could've recognised Mr C was the potential victim of a scam based on what he told it – that he was paying his builder. But I disagree - thinkmoney's own website talks about the importance of every customer verifying any information it receives via email. It doesn't go into detail about this particular scam, but it does direct its customers to a third party government website which does provide details of invoice scams and how individuals can protect themselves from them. It sets out that this type of scam is characterised by someone's builder contacting victims with amended bank details requesting payment.

I can also see that as far back as 2016, the Financial Conduct Authority, Actionfraud and various media platforms have published information online about email and invoice intercept scams and how they tend to be perpetrated. So I don't accept this scam isn't common or well known as thinkmoney has suggested.

Thinkmoney has said even if it had adequately questioned Mr C and warned him about this type of scam and how it's commonly perpetrated, it wouldn't have made a difference. But, if thinkmoney had sufficiently warned him about how this type of scam tends to work, given all it would take to verify the details is a call or message to his builder via his son, I'm not sure on what basis thinkmoney believes Mr C wouldn't have done this. I think any reasonable person would likely carry out this additional check to avoid the potential loss of £10,000.

Overall, based on the evidence and information available to both thinkmoney and Mr C at the time the payment was made, I think it's likely Mr C wouldn't have made the payment he did to the scammer. As thinkmoney has missed an opportunity to stop the payment being made, I think it's liable for his loss.

I've also considered in this case whether I think Mr C shares any liability for his loss by way of contributory negligence. But from the evidence he's provided it appears that the scammers accessed the builder's genuine email account to send correspondence to Mr C's son (who was dealing with the situation on Mr C's behalf). The email the scammer sent seems to reflect the amount required as a deposit they'd previously agreed, the email address and signature were genuine and the language and writing style were in line with other emails. And, the payment was being requested on the date Mr C had expected to pay it.

Overall, I don't think anything stood out in the email requesting payment that ought to have seemed unusual or an obvious sign of a scam to Mr C or his son given I wouldn't expect either to have an in depth knowledge of common fraud and scams and how they tend to be perpetrated. I don't think Mr C shares any liability for the loss in this case.

Thinkmoney has acknowledged it didn't respond to Mr C's contact regarding the fraud as soon as it could've. Mr C has also said he had some difficulty contacting it over the phone and needed to report the scam via social media channels. I can see this would've been frustrating given the stress he was under at the time. Overall I think the £50 thinkmoney has offered is sufficient compensation.

Putting things right

Think Money Limited should reimburse Mr C the £10,000 he lost as a result of a scam. It should apply interest to this amount at a rate of 8% from the date of payment to the date of settlement.

If it hasn't already it should also pay Mr C the £50 compensation offered for the customer service provided.

My final decision

I uphold this complaint and require Think Money Limited to pay the redress outlined above. Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 22 August 2022.

Faye Brownhill
Ombudsman

